

Audit



Report

OFFICE OF THE INSPECTOR GENERAL

**FEDERAL ACQUISITION COMPUTER
NETWORK CENTRAL CONTRACTOR
REGISTRATION (CCR) PROGRAM**

Report No. 98-012

October 22, 1997

DISTRIBUTION STATEMENT A
Approved for Public Release
Distribution Unlimited

19991007 065

Department of Defense

DTIC QUALITY INSPECTED 4

ART 00-01-0016

Additional Copies

To obtain additional copies of this audit report, contact the Secondary Reports Distribution Unit of the Analysis, Planning, and Technical Support Directorate at (703) 604-8937 (DSN 664-8937) or FAX (703) 604-8932.

Suggestions for Future Audits

To suggest ideas for or to request future evaluations, contact the Planning and Coordination Branch of the Analysis, Planning, and Technical Support Directorate at (703) 604-8908 (DSN 664-8908) or FAX (703) 604-8932. Ideas and requests can also be mailed to:

OAIG-AUD (ATTN: APTS Audit Suggestions)
Inspector General, Department of Defense
400 Army Navy Drive (Room 801)
Arlington, Virginia 22202-2884

Defense Hotline

To report fraud, waste, or abuse, contact the Defense Hotline by calling (800) 424-9098; by sending an electronic message to <hotline@dodig.osd.mil>; or by writing the Defense Hotline, The Pentagon, Washington, D.C. 20301-1900. The identity of each writer and caller is fully protected.

Acronyms

CAGE	Commercial and Government Entity
CCR	Central Contractor Registration
DFAR	Defense Federal Acquisition Regulation
DFAS	Defense Finance and Accounting Service
DISA	Defense Information Systems Agency
DLSC	Defense Logistics Supply Center
DUNS	Data Universal Numbering System
EC	Electronic Commerce
ECPN	Electronic Commerce Processing Node
EDI	Electronic Data Interchange
EFT	Electronic Funds Transfer
FACNET	Federal Acquisition Computer Network
FAR	Federal Acquisition Regulation
PASS	Procurement Automated Source System
SSL	Secure Sockets Layer
VAN	Value-Added Network



**INSPECTOR GENERAL
DEPARTMENT OF DEFENSE
400 ARMY NAVY DRIVE
ARLINGTON, VIRGINIA 22202-2884**



October 22, 1997

MEMORANDUM FOR DEPUTY UNDER SECRETARY OF DEFENSE
(LOGISTICS)
ASSISTANT SECRETARY OF THE NAVY (FINANCIAL
MANAGEMENT AND COMPTROLLER)
ASSISTANT SECRETARY OF THE AIR FORCE
(FINANCIAL MANAGEMENT AND COMPTROLLER)
DIRECTOR, DEFENSE PROCUREMENT
DIRECTOR, DEFENSE FINANCE AND ACCOUNTING
SERVICE
DIRECTOR, DEFENSE INFORMATION SYSTEMS
AGENCY
AUDITOR GENERAL, DEPARTMENT OF THE ARMY

SUBJECT: Audit Report on Federal Acquisition Computer Network Central Contractor
Registration (CCR) Program (Report No. 98-012)

We are providing this audit report for your review and comment. We considered management comments on a draft of this report in preparing the final report.

DoD Directive 7650.3 requires that all recommendations and potential monetary benefits be resolved promptly. As a result of management comments, we deleted Recommendations A.6.a. and redirected Recommendation A.6.c. to the Director, Defense Finance and Accounting Service, as Recommendation A.7. We request that the Director, Defense Finance and Accounting Service, provide comments on this additional recommendation by November 24, 1997.

We appreciate the courtesies extended to the audit staff. Questions on the audit should be directed to Ms. Kimberley A. Caprio, Audit Program Director, at (703) 604-9140 (DSN 664-9140), email <kcaprio@dodig.osd.mil> or Mr. Kent E. Shaw, Audit Project Manager, at (703) 604-9228 (DSN 664-9228), email <kshaw@dodig.osd.mil>. See Appendix E for the report distribution. The audit team members are listed inside the back cover.

Robert J. Lieberman
Assistant Inspector General
for Auditing

Office of the Inspector General, DoD

Report No. 98-012

(Project No. 6CA-0070)

October 22, 1997

Federal Acquisition Computer Network Central Contractor Registration (CCR) Program

Executive Summary

Introduction. The Federal Acquisition Regulation requires contractors to register with the Central Contractor Registration (CCR) program office before doing business electronically with the Federal Government. The Debt Collection Improvement Act of 1996 requires Federal agencies to have the Taxpayer Identification Number of every contractor and pay every contractor through electronic funds transfer. Having the necessary contractor information centrally located and available to both contracting and payment offices through the CCR will greatly enhance the ability of DoD to comply with the law. Information contained in the CCR database is also needed to comply with Internal Revenue Service reporting requirements.

Audit Objectives. The primary audit objectives were to evaluate the progress that the Electronic Commerce Integration Organization and its predecessor, the DoD Electronic Commerce Office, and the Defense Information Systems Agency have made in implementing the CCR Program, to determine why few contractors have registered, and to review access controls over sensitive contractor information contained in the CCR database. We also examined the management control program as it relates to the audit objective. See Appendix A for a discussion of the audit scope and methodology and for a summary of prior coverage related to the audit objectives.

Audit Results. Progress in centrally registering contractors who wish to do business with DoD has been disappointingly slow. Only 3.3 percent of about 400,000 potential Government contractors have registered with the CCR Program since the program was initiated in December 1994. As a result, the vision of using a single method of collecting contractor information is not being realized, the ability to use the data for electronic payment and Internal Revenue Service reporting is at risk, and contractors are not in compliance with Federal Acquisition Regulation requirements to register with the CCR before conducting electronic commerce over FACNET. Although DoD has made progress in improving security over FACNET and protecting the CCR data, security needs further improvement. Without the additional protection provided by systems that provide Controlled Access Protection, an additional firewall, and a secure web server, CCR data will be subject to increased risk of improper access or disclosure of sensitive information. See Part I for a discussion of the audit results and see Appendix A for details on the management control program.

Summary of Recommendations. We recommend that the Executive Director, Electronic Commerce Integration Organization, conduct expedited cost effectiveness and technical assessment studies for using existing databases to populate the CCR database; use CD-ROM disks or alternative electronic means to distribute CCR data to DoD contracting offices and payment offices until all users are provided a capability to read the data using FACNET; and develop training courses on access and use of the Central Contractor Registration database. We recommend that the Director, Defense Procurement:

- Develop an information package on the CCR Program and encourage DoD small business offices and contracting offices to provide the information packages to potential contractors.
- Direct the Service Senior Acquisition Executives to upgrade their contracting equipment and software to access the CCR database.
- Require that all Defense contracting officers obtain training in access and use of the CCR database.
- Publish information on the requirement to register for CCR in the Commerce Business Daily.

We recommend that the Director, Defense Finance and Accounting Service develop the necessary interfaces in Defense Finance and Accounting Service automated systems to use the CCR data for Internal Revenue Service Form 1099 generation and electronic payment of funds to DoD contractors.

We recommend that the Director, Defense Information Systems Agency upgrade the CCR operating system to comply with network security requirements of DoD Directive 5200.28; install a firewall that will restrict access to the CCR Interface computer; and install security software for its Internet web server that will encrypt registration data.

Management Comments. We received comments from the Under Secretary of Defense for Acquisition and Technology, Executive Director, Electronic Commerce Integration Organization; Under Secretary of Defense for Acquisition and Technology, Director, Defense Procurement; Director, Defense Information Systems Agency; and the Commander, Military Traffic Management Command. We did not receive comments from the Defense Finance and Accounting Service. Management generally agreed with all of our recommendations. See Part I for summary of management comments and Part III for the complete text of management comments.

Additional Comments Required. The Defense Finance and Accounting Service is requested to provide comments by November 24, 1997.

Table of Contents

Executive Summary	i
Part I - Audit Results	
Audit Background	2
Audit Objectives	6
Finding A. Progress of the Central Contractor Registration	8
Finding B. CCR Data Access Protection	25
Part II - Additional Information	
Appendix A. Audit Process	
Scope	34
Management Control Program	35
Appendix B. Summary of Prior Coverage	36
Appendix C. Summary of Data Elements	42
Appendix D. Glossary	44
Appendix E. Report Distribution	46
Part III - Management Comments	
Under Secretary of Defense for	
Acquisition and Technology Comments	50
Department of the Army Comments	56
Defense of Defense Information Systems Agency Comments	58

Part I - Audit Results

Audit Background

Central Contractor Registration Program. The concept of a Central Contractor Registration (CCR) program was initially proposed in the mid-1980s by the Procurement Automation Council, an interagency group led by the Office of Federal Procurement Policy. In the late 1980s, the Director, Defense Procurement sponsored studies by the Logistics Management Agency that culminated in recommendations to implement the central registration concept. A 1993 report¹ prepared by a process action team established by the Deputy Under Secretary of Defense (Acquisition Reform) (DUSD[AR]) proposed the development of the CCR as part of the Federal Acquisition Computer Network (FACNET). The intent of the CCR was to simplify the registration process for contractors by requiring them to register only once to do business with the Government rather than registering separately with each Government procurement office. In addition to making it easier for contractors to do business with the Government, other objectives of developing the CCR were to serve as a source to update the individual Federal agency's procurement systems, to establish unique identifier codes for each contractor (and major components of the contractor), and to update contracting officers' bidder's mailing lists.

Congress directed the development of FACNET in the Federal Acquisition Streamlining Act of 1994. The act required the development of FACNET and electronic generation and transmission of procurement transactions between the Government and its contractors Government-wide by January 2000. Federal Acquisition Regulation (FAR) section 4.503, Contractor Registration, requires contractors to register with the CCR program before doing electronic commerce over FACNET.

The Federal Acquisition Reform Act of 1996, eliminated the requirement for individual Government contracting offices to become interim FACNET certified² to use simplified acquisition procedures for purchases valued up to \$100,000. This change allowed all contracting officers to take advantage of the increased simplified acquisition threshold. According to the FAR, any contracting activity wanting to engage in Electronic Commerce is still required

¹ DoD Electronic Commerce (EC)/ Electronic Data Interchange (EDI) in Contracting Report, December 20, 1993.

² Interim FACNET certified means that the contracting office must electronically provide widespread public notice of solicitations for contract opportunities; receive responses to solicitations and associated requests for information; allow private sector users to access notice of solicitations for contract opportunities, access and review solicitations, and respond to solicitations issued by a contracting office; and issue notices of solicitations and receive responses to solicitations in a system having those functions.

to become interim FACNET certified pursuant to FAR section 4.505. However, the Act did not eliminate the requirement of contractors to register with the CCR.

Other Uses of CCR. The CCR data is also intended to help DoD comply with new requirements under the Debt Collection Improvement Act of 1996 and to comply with Internal Revenue Service requirements to report annual contractor payments.

The Debt Collection Improvement Act of 1996 requires Federal agencies to electronically pay all the contractors they trade with by January 1, 1999. Data in the CCR registration database (bank accounts, bank routing information, and taxpayer identification numbers) will be critical to meeting the Act's requirements. Having the necessary contractor information centrally available through the CCR, where it can be accessed by both contracting and payment offices, will greatly enhance the ability of DoD to pay contractors electronically. The Act provides an opportunity for the Federal Government to move toward its goal of electronic commerce and efficient cash and debt collection management.

In addition, the Internal Revenue Service Regulations require Federal agencies to report payments for services obtained from noncorporate contractors, and some medical service corporations, when the costs of those services total \$600 or more in a calendar year. This information is reported by the DoD payment offices to the Internal Revenue Service on Internal Revenue Service Form 1099-Misc, Miscellaneous Income. Additionally, Internal Revenue Code section 6050M requires the reporting of all government contracting actions over \$25,000 to the Internal Revenue Service. Information contained in the CCR registration database, such as taxpayer identification number, corporate address, and type of commercial entity is needed to satisfy those reporting requirements.

Responsibility for Central Contractor Registration. Until February 19, 1997, the DUSD(AR) was the executive agent for FACNET and the CCR. The DUSD(AR) delegated overall program responsibility and accountability to the Director, DoD Electronic Commerce. As program manager, the Director, DoD Electronic Commerce, was responsible for the following:

- funding and managing the implementation of the CCR Program,
- facilitating the development of functional policy,
- identification and validation of requirements,
- chairing the CCR Joint Configuration Control Board,

- oversight of the population of CCR, and
- monitoring performance.

On February 19, 1997, the Principal Deputy Under Secretary of Defense for Acquisition and Technology issued a memorandum directing the transfer of Electronic Commerce/Electronic Data Interchange (EC/EDI) responsibility, including the CCR, from DUSD(AR) to DUSD(Logistics). The responsibilities of the DoD Director, Electronic Commerce were subsequently assigned to the Executive Director, Electronic Commerce Integration Organization.

The Defense Information Systems Agency (DISA) is responsible for CCR technical operations and software development including security policy; physical security; systems administration; backup and recovery of CCR data; data transmission; hardware and software configuration; documentation of the CCR system; and software design, development, and testing. On November 18, 1996, the Defense Logistics Supply Center (DLSC) assumed responsibility for CCR customer support including data dissemination, customer service, and education and outreach.

As shown in Figure 1, contractors can obtain information on how to register for the CCR from the Electronic Commerce Information Center. The contractor must also request a Commercial and Government Entity (CAGE) code from DLSC and request a Data Universal Numbering System (DUNS) number from Dunn and Bradstreet. The CCR requires that the contractors provide up to 60 data elements in order to register. (See Appendix C.)

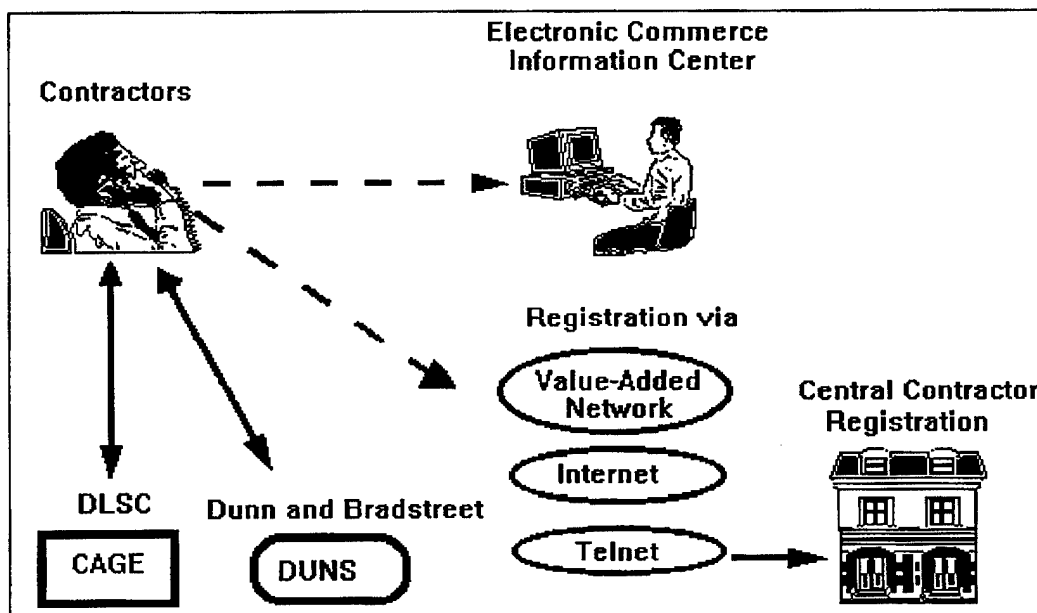


Figure 1. Central Contractor Registration Process

As of August 15, 1997, 13,236 contractors had registered with the CCR program. According to the Directorate for Information Operations and Reports at Washington Headquarters Services, the universe of contractors that do business with the Government numbers at least 400,000.

As shown in Figure 2, contractors can register with the CCR program by submitting the information through a Value-Added Network (VAN) or by entering the information through an Internet web browser. In addition, contractors can also register with the CCR program by submitting the information through telefacsimile.

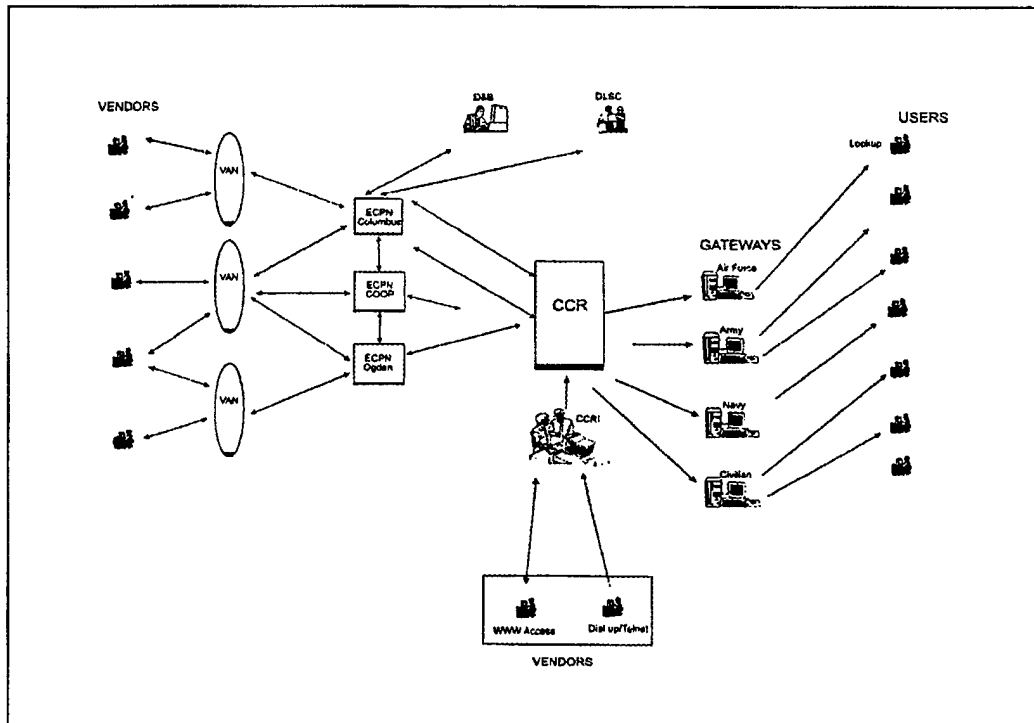


Figure 2. CCR Infrastructure (Source: Director, DoD Electronic Commerce)

Central Contractor Registration Process Via VAN. Contractors can submit a CCR registration to a commercial entity known as a VAN. The VAN provides connections to FACNET and technical support to its customers. The VAN also converts information received from the contractor to a standard format and transmits the data over FACNET to the CCR database in Columbus, Ohio.

Central Contractor Registration Via Internet and Telefacsimile.

Contractors can also submit registration information to the CCR via an Internet web server. Internet web servers are computers that provide a graphical interface between the users and a host computer. Internet registration allows contractors to submit data directly to the CCR database without going through a

VAN. The use of an Internet web page to collect the CCR information by the CCR Program is a recent development that began October 1, 1996. Contractors can also send their application to CCR by telefacsimile.

Validation of CCR Data. Once the information is received by the CCR database an extract of the submitted information is transmitted to DLSC and Dunn and Bradstreet for validation. Once the data is validated the contractor registration process is complete.

CCR Data Storage. DISA uses two computers to store the CCR data for security reasons. The first computer, known as the CCR machine, in Columbus, Ohio, is used to process registrations, separately store registrations that have been submitted but are not yet validated, and to store valid CCR registrations. The Electronic Commerce Processing Node (ECPN) is the only point of entry into the CCR machine. The CCR machine is also used for distribution of valid CCR registrations to FACNET users and to the Central Contractor Registration Interface (CCRI). The CCR machine is isolated from the Internet while the CCRI is used to interface with Internet users. Internet users can enter or update registration information into CCRI or query CCRI's copy of valid CCR data. Internet users also have the option of holding an incomplete registration on CCRI until they can obtain all their information required for registration. New or updated registrations submitted on CCRI are not processed until they are sent from CCRI through the ECPN to the CCR machine, the second computer.

CCR Security Implications. Registering with CCR eliminates the need for many of the paper documents otherwise required for contractor registration. As a result, original hard copy evidence of the registration may not be available. Instead, electronic records must be used. CCR data become electronic records as they are prepared for transmission and when they are received. Security must be established to assure that CCR data, as electronic records, are authentic and properly authorized, and are reliably carried from their source to their destination. In addition, CCR data, while being communicated or stored as records, must be protected from loss, modification, or unauthorized disclosure. Eight of the 60 data elements included in the CCR program require strict access control and are not releasable to the public.

Audit Objectives

The primary audit objectives were to evaluate the progress that the (Executive Director, Electronic Integration Organization) Director, DoD Electronic Commerce and the DISA have made in implementing the CCR program; to determine why few contractors have registered; and to review access controls over sensitive contractor information contained in the program's data base. We

also examined the management control program as it relates to the audit objectives. See Appendix A for a discussion of the scope, methodology, and management control program. Appendix B summarizes prior coverage related to the audit objectives.

Finding A. Progress of the Central Contractor Registration

Progress in populating the CCR has been disappointingly slow. The CCR program was initiated in December 1994. Since that date, only 13,236 or approximately 3.3 percent of about 400,000 potential Government contractors have registered with the CCR program. Additionally, many of the potential users of CCR are unable to use, or are not using, the CCR data for contracting. Therefore, progress has been slow in implementing a fully-functional CCR program. Progress has been slow in populating the CCR because the Director, DoD Electronic Commerce has not made maximum use of existing data to populate the CCR database; and DoD small business offices and contracting offices are not promoting the CCR program.

- DoD organizations are not using the CCR program because:
 - aged computer equipment in the DoD contracting offices is unable to access or use the CCR data;
 - agency applications are not designed to use the data;
 - DoD contracting personnel have not received training on how to use CCR data;
 - most DoD contracting offices continue to operate contractor registration systems separately from the CCR;
- DFAS only recently began determining its data requirements; and
- the DFAS has not developed the necessary interface to use the CCR data for electronic payment and Internal Revenue Service reporting.

As a result, the vision of a single method of collecting and centralizing standardized contractor information to eliminate duplication and inefficiency is not being realized. Also, the ability to use the data for electronic payment and preparation of required Internal Revenue Service forms is at risk. Finally, contractors are not in compliance with Federal Acquisition Regulation 4.503 requirements.

Central Contractor Registration Mandate

Federal Acquisition Regulation 4.503, Contractor Registration, requires that all contractors who participate in electronic commerce with the Federal Government register with the CCR. The Federal Electronic Commerce Acquisition Instruction, March 10, 1995, requires that contractors register in the CCR to establish a trading-partner relationship with the Government; or to conduct business with Federal Government agencies using EC/EDI technologies including FACNET, or manual procurement methods.

The Director of Defense Procurement policy memorandum, Central Contractor Registration, February 10, 1997, required that all contractors that respond to solicitations issued after September 30, 1997, be registered in the CCR before they can be awarded a contract. This requirement applied to all solicitations and awards whether performed electronically or not. The memorandum only excluded:

- purchases made with Government-wide commercial purchase cards;
- contracting officers located outside the U.S.;
- classified contracts; and
- contracts executed to support contingency or emergency operations.

The memorandum further directed DoD contracting offices to take whatever actions necessary to inform contractors of the new requirement. On June 11, 1997, the Under Secretary of Defense (Comptroller) and the Director, Defense Procurement issued a joint memorandum extending this deadline to March 31, 1998.

Progress of Central Contractor Registration

As of August 15, 1997, only 13,236 contractors, or approximately 3.3 percent of about 400,000 potential Government contractors, have registered with the CCR program. The total number of contractors was estimated, based on information provided to us by the Washington Headquarters Services, Directorate for Information Operations and Reports. Our estimate may be lower than the actual number of contractors because the data we used only included those contractors with contractual actions of \$25,000 or larger. Although the number of contractors that have registered has steadily increased since the program began (see figure 3), the progress is not rapid enough to meet Federal and DoD mandates on CCR. A potential 387,000 additional contractors must register by March 31, 1998, in order to be awarded contracts.

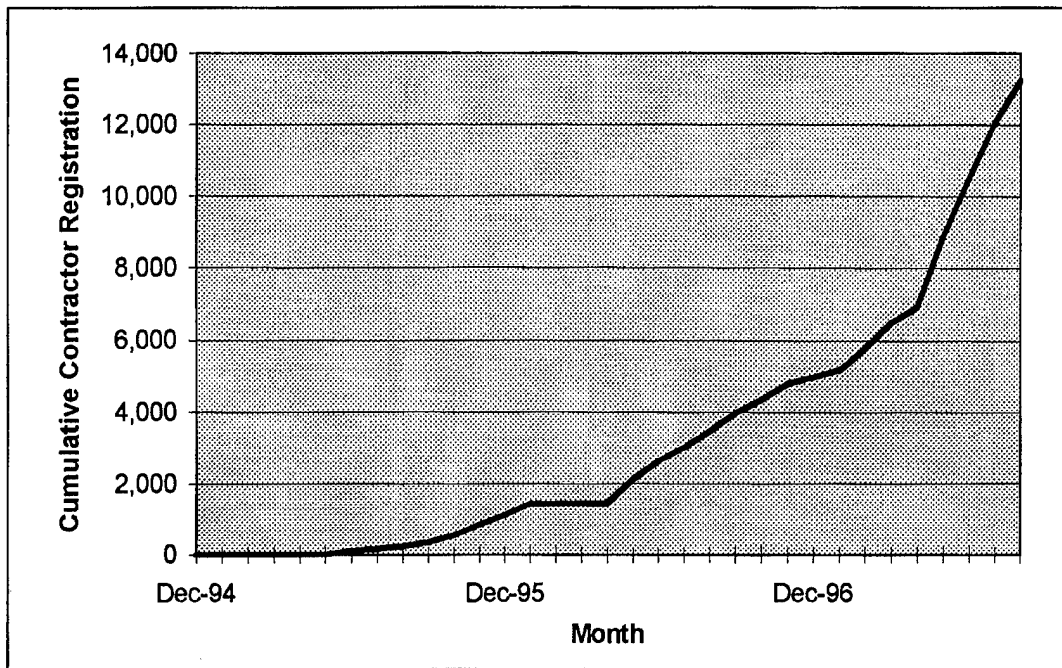


Figure 3. Progress in CCR Registration

Use of Existing Data to Populate the CCR

Existing Databases. The Director, DoD Electronic Commerce, has not used existing contractor data effectively to populate the CCR database. Currently contractors must supply up to 60 items of information to register for the CCR. The Director, DoD Electronic Commerce, estimated that it takes about 45 minutes to supply all of the data elements. The information can be sent to the CCR through the Internet, VAN or mail. The registration process takes 7-10 days if submitted via Internet or VAN, and approximately 30 days if mailed.

We compared each of the 60 data elements required for the CCR with data available in other commercial and Government-owned databases (see Appendix C). Fifty percent of the data elements being solicited from the contractors for CCR registration was already available. For example, data to populate the CCR is readily available from the following sources.

Contracting Officers' Bidder Lists. Contracting officers typically maintain a collection of bidders derived from the Standard Form 129, Solicitation Mailing List Application. The form includes up to 14 data elements needed in the CCR. We could not determine the total number of such records, but obtaining these databases from some of the larger contracting officers could be a beneficial source for populating the CCR database.

Finding A. Progress of the Central Contractor Registration

Small Business Administration Procurement Automated Source System (PASS) Database. The Small Business Administration currently maintains a database of small businesses interested in Federal Government opportunities. The Small Business Administration's PASS contains about 197,000 sources. The PASS database contains 22 data elements needed in the CCR database.

Defense Logistics Supply Center Commercial and Government Entity Code Database. Defense Logistics Supply Center (DLSC) currently performs a function similar to the CCR in support of the Federal Logistics Information System and acts as the single location for obtaining a CAGE code. Federal Logistics Information System is a data acquisition, validation and distribution mechanism. The CAGE database contains 17 data elements needed in the CCR database. There are about 55,000 parent company records in the DLSC CAGE database.

DoD Individual Contracting Action Report. In FY 1979 the Defense Contract Action Data System became the official means of DoD contractor data collection for the Federal Procurement Data System. This automated system collects data from DD Form 350, Individual Contracting Action Report, and DD Form 1057, Monthly Contracting Summary Actions of \$25,000 or less. The Director, Defense Procurement is responsible for this data collection system, which has been in existence within DoD for over 30 years. The database contains 13 data elements needed in the CCR database and consists of records on about 400,000 contractors.

Dunn and Brad Street's DUNS. Dunn and Bradstreet currently maintains a database containing approximately 41 million records. The Dunn and Bradstreet database contains four data elements needed in the CCR. The Federal Electronic Commerce Acquisition Team recommended the use of the DUNS number as the contractor identification code for electronic commerce.

Taxpayer Identification Numbers. Contractors are required by the Internal Revenue Service to provide taxpayer identification numbers when requested by contracting offices on Internal Revenue Service form W-9, Request for Taxpayer Identification Number and Certification. The form is a self-certification of a contractor's mailing address, taxpayer identification number, and type of business. If authorized, the data could be beneficial in populating some of the CCR database. The form contains 8 data elements needed in the CCR database.

Use of Alternative Databases. Although our audit did not test the accuracy of the data in the existing databases, we believe that progress in registering contractors for the CCR can be significantly improved by initially populating the CCR database with existing information. Subsequently, that information could be mailed to contractors for updates and addition of any missing data elements. Technical assistance in compilation of the data from the existing databases can be obtained through contracts with companies that specialize in mass mailing. Such contractors are experts in compiling and purifying database

Finding A. Progress of the Central Contractor Registration

information. The Executive Director, Electronic Commerce Integration Organization could then validate the data using the current validation process.

The former Director, DoD Electronic Commerce, chose not to use existing information because of technical difficulty and cost involved in combining other data elements. Also, some Government owners of other databases did not want to assist the Director in populating the CCR because of fear of sacrificing their own databases. The Executive Director, Electronic Commerce Integration Organization should conduct an expedited cost effectiveness study and technical assessment of use of existing databases to populate the CCR database.

Recent Effort To Use Alternative Contractor Data. In April 1997, the Director, DoD Electronic Commerce, and McDonnell Douglas Corporation co-authored a letter to McDonnell Douglas's 4,500 preferred suppliers advising them of DoD policy for registration and McDonnell Douglas's support of DoD as a prime contractor. Additionally, the Small Manufacturer's Association of California, representing about 10,000 small businesses in the state, has volunteered to assist in dissemination of the information to their members. The Director, DoD Electronic Commerce briefed approximately 1,500 additional DoD industry participants, facilitated their understanding of new policy, and explained how they individually could utilize the DoD Electronic Commerce CCR Assistant Center. A total of 16,000 small and medium-sized businesses have received information directly from these initiatives.

Promoting CCR Program

DoD Small and Disadvantaged Business Utilization Offices and contracting offices are not promoting the CCR program. These offices have not established and implemented a policy to promote the CCR program. Instead, they require only that contractors submit a Standard Form 129, Solicitation Mailing List Application for registration with that office. In addition, some contracting offices require DD Form 2051, Request for Assignment of a Commercial and Government Entity (CAGE) Code, to be considered for registration with that office. Since these offices are often the primary source for information on Government contracting, we believe that the contractors should be informed of the CCR and provided with registration information for the CCR. Additionally the Director, Defense Procurement should periodically publish information on the requirement to register for the CCR in the Commerce Business Daily.

Use of CCR Data for Contracting

Obsolete Computer Equipment. DoD contracting offices are not able to use CCR data because their computer equipment is too old to access the data due to memory capacity and hardware architecture. For example, the Air Force uses Wang computers purchased in the 1980's at its contracting offices. Wang computers are based on obsolete Intel 286 processors. These computers can not run the Windows-based applications needed to use Internet utilities to access the CCR database.

Problems using CCR data with obsolete computer equipment are also recognized by the top DoD Acquisition Executive, the Under Secretary of Defense for Acquisition and Technology. On December 14, 1996, the Under Secretary of Defense for Acquisition and Technology issued a memorandum to the Component Acquisition Executives concerning electronic access to acquisition reform information and training materials. The memorandum states that, in spite of the large installed base of information technology in acquisition organizations, the entire acquisition workforce is not yet in the electronic age of the late-1990's. Ability to reach everyone electronically, in a user friendly manner, remains an elusive but important goal. Acquisition workforce professionals need the ability to receive and send email messages, access to the Web, and CD-ROM capability. The Under Secretary of Defense for Acquisition and Technology stated full capability will entail hardware and software that fully supports individual use of the Web and CD-ROM; unimpeded, reliable access to the Web down to the individual level; ability to connect and transfer data at rates fast enough to support use of the web; and command policy on individual access to the Internet consistent with security needs. In conclusion, the Under Secretary of Defense for Acquisition and Technology stated that education and training must be a priority at all levels of the workforce. Additionally, management must actively lead and participate in structuring an effective education and training program.

Software Not Designed to Read CCR Data. The types of contracting software used by DoD contracting offices are not designed to receive all CCR data elements. For example, an Air Force system can only receive 22 of 60 data elements. The Navy system can not receive any data elements electronically. Therefore, the Navy contracting offices receive a hard copy of CCR data from the CCR database in Columbus, Ohio, and manually input the data into their system. Currently Government procurement systems are not required by the Federal Acquisition Regulation to be able to read the standard record format for CCR data to obtain interim FACNET certification.

Training for Using CCR Data. DoD does not train its contracting officers on access and use of CCR data. DoD contracting officials and training officials from the Defense Acquisition University unanimously agreed that there is no

Finding A. Progress of the Central Contractor Registration

CCR training requirement for contracting personnel. Training would ensure that contracting officers are aware of and capable of using the CCR. The DISA should establish courses to train contracting officers to access and use the CCR database.

Separate Efforts to Register Contractors. As a result of the problems discussed above, DoD contracting offices require contractors to register in individual DoD contracting offices' own locally developed contractor database to select contractors. Contractors generally register by submitting the U.S. Government Standard Form 129 prepared by the General Services Administration. Table 1 shows 12 locally developed contractor databases we judgmentally selected, and the number of contractors registered with their databases.

Finding A. Progress of the Central Contractor Registration

Table 1. Locally Developed Contractor Database

Contracting Offices	Locally Developed Contractor Database	Number of Contractors Registered
Fort Bliss	Standard Army Automated Contracting Systems	6,809
Fort Gordon	Standard Army Automated Contracting Systems	5,278
Fort Sam Houston	Standard Army Automated Contracting Systems	13,137
Military Traffic Management Command	Carrier Qualification Program	1,800
Tank-Automotive and Armaments Command	Direct Vendor Delivery program	60
Engineering Field Activity, Midwest	Standard Automated Contracting Systems	3,600
Naval Surface Warfare Center, Crane, IN	Industrial Logistics Support Management Information System	32,500
National Naval Medical Center	Standard Automated Contracting System	2,300
Navy Inventory Control Point, Philadelphia, PA	Integrated Technical Item Management Procurement	14,000
Charleston AFB	Base Contracting Automated System	4,500
McConnell AFB	Base Contracting Automated System	7,400
Scott AFB	Base Contracting Automated System	7,500
Total		98,884

Finding A. Progress of the Central Contractor Registration

Even though DoD has spent \$81.5 million to fund Electronic Commerce Resource Centers to promote contractor use of electronic commerce for the last two years³, all contracting officials for 12 locally developed contractor databases stated that the CCR database is not populated enough to select contractors, is cumbersome, and is generally not useful in its present condition.

The Director, Defense Procurement should require that all DoD contracting offices upgrade their contracting equipment and software for accessing CCR; DoD contracting officers be trained in access and use of the CCR database; and all DoD contracting officers use CCR to award any contracts to prospective contractors. Until the DoD contracting offices are capable of reading the CCR data over a network, the Executive Director, Electronic Commerce Integration Organization should develop an alternative method of distributing the CCR data, such as CD-ROM disks.

Use of CCR Data for Electronic Payment and Tax-Related Information Reporting

Two intents of the CCR program were to facilitate use of Electronic Funds Transfer (EFT) for contract payments, and to help payment offices prepare reports of contract payments to Internal Revenue Service. The Defense Finance and Accounting Service (DFAS) is responsible for developing the CCR financial data elements for DFAS use in centralized EFT processing and Internal Revenue Service reporting requirements. The DFAS began participation in development of its data requirements during November 1996. These data requirements were finalized during March 1997. As a result of DFAS late involvement in the CCR program, the DFAS has not developed the necessary interface to use the CCR data for EFT and Internal Revenue Service reporting.

Electronic Funds Transfer. Successful registration of all contractors is critical to DoD compliance with the recently enacted Debt Collection Improvement Act of 1996. This Act requires Federal Agencies to have the Taxpayer Identification Number of every contractor they do business with, and to pay contractors through electronic funds transfer. Having the necessary contractor information centrally available through the CCR, where it can be accessed by both contracting and payment offices, will facilitate DoD compliance with the law.

³Inspector General, DoD, Report No. 97-090, Electronic Commerce Resource Centers, February 11, 1997. This report stated that DoD obligated approximately \$81.5 million for FY 1994 through the first quarter of FY 1996 that did not greatly increase the implementation and use of EC/EDI technologies. The report is summarized in Appendix B.

Finding A. Progress of the Central Contractor Registration

Internal Revenue Service Reporting. Contractor registration in the CCR is critical to DoD ability to satisfy Internal Revenue Service reporting requirements. DoD is required to prepare Internal Revenue Service Form 1099-Misc, Miscellaneous Income, for all noncorporate contractors and some medical service corporations that are paid more than \$600 each year. Also, under Internal Revenue Code section 6050M, all Government contracting actions over \$25,000 must be reported to the Internal Revenue Service through the Federal Procurement Data Center. The Internal Revenue Service uses the Form 1099 reports to identify unreported income by the contractors who receive those funds. Contractual actions reported by the Federal Procurement Data Center are used by the Internal Revenue Service to identify potential offsets for any delinquent taxes owed by the contractors. Recently, two reports were issued on noncompliance with the Internal Revenue Service reporting requirements. Additionally, we found that about \$3 billion was not being properly reported to the Internal Revenue Service as required under the 6050M because the taxpayer identification numbers were missing. Also the Military Traffic Management Command was not performing the required 6050M reporting for personal property carriers and freight carriers. As a result of not reporting or inaccurately reporting the required information to the Internal Revenue Service, the Internal Revenue Service may suffer a reduced level of taxpayer compliance and may not be able to offset delinquent tax liabilities with Government contract payments.

Inspector General, DoD, Report. Inspector General, DoD, Report No. 95-234, DoD Compliance with Federal Tax Reporting Requirements, June 14, 1995, found that overall DoD management of the Internal Revenue Service Form 1099 reporting process was inadequate. Specifically, 10 of the 11 DoD paying offices visited were not obtaining needed information, maintaining accurate records, or reporting payments for noncorporate contractors and certain medical service corporations. This condition existed because DoD contracting offices did not always provide DoD paying offices with the taxpayer information that was needed to perform Internal Revenue Service Form 1099 reporting. The report recommended that the Under Secretary of Defense for Acquisition and Technology enforce compliance with the FAR 52.204-3 and 4.203, which require contracting officers to obtain taxpayer identification numbers, corporate status, and the contract type for all procurement actions, regardless of dollar value; and submit the information to the paying office. The Director, Defense Procurement concurred and stated that the DoD will achieve compliance with the FAR requirements via CCR registration of all contractors that do business with DoD. The Director, Defense Procurement anticipated that CCR will be substantially complete within 2 years.

Office of Management and Budget Report. The Office of Management and Budget Report to the Congress, Improvements Needed in Federal Agency Tax-Related Information Reporting to Ensure Tax Compliance of Federal Contractors, April 1, 1994, concluded that Federal agencies were not complying with Internal Revenue Service Form 1099 reporting requirements; and that 22 percent of the contractors doing business with the Government owed delinquent taxes. The report recommended that Federal agencies:

Finding A. Progress of the Central Contractor Registration

- take immediate steps to check contractors' tax compliance;
- certify that procedures and policies are in place by March 30, 1995, to meet Internal Revenue Service Form 1099 reporting requirements; and
- ensure that the required taxpayer identification numbers are obtained and verified.

Unreported and Improperly Reported Income. For FY 1996, DoD reported \$122.9 billion in contractual actions to the Federal Procurement Data Center. This information is compiled from the DD Form 350, Individual Contracting Action Report, which is prepared by the contracting officer for each contractual action over \$25,000. To test the accuracy of the data, we requested the Washington Headquarters Services to summarize all reports that had missing taxpayer identification numbers. After eliminating foreign corporations and other inter-government transactions, we determined that contracting actions totaling about \$3.0 billion were missing the required taxpayer identification numbers. If the taxpayer identification numbers for all DoD contractors were readily available in the CCR to those contracting officers who prepare the DD Form 350, we believe that the accuracy of the data could be improved and its value to the Internal Revenue Service increased.

The DFAS was not reporting the contractual actions over \$25,000 for personal property carriers and freight carriers as required. The personal property and freight carriers are paid about \$1.4 billion each year. Although we expect the number of Military Traffic Management Command transactions over \$25,000 to be low, compliance is still required. To comply with the Internal Revenue Service Reporting requirements, the Military Traffic Management Command needs to require that its personal property carriers and freight carriers are registered in the CCR system; and the DFAS needs to prepare and submit the DD 350 report for each contractual action of \$25,000 or more to the Washington Headquarters Services.

DFAS participation in CCR. DFAS officials stated that concerns about insufficient security for CCR financial information has impeded their participation in implementing the CCR. DFAS officials also expressed concern about the capability of the CCR database in handling the DFAS volume of invoices and transactions (about 100,000 per day). In addition, DFAS has not received guidance on how to implement EFT and Internal Revenue Service reporting for the CCR program. Therefore, DFAS is not currently using CCR data for centralized processing of EFT to pay contractors. However, in March 1997, DFAS began developing financial data elements needed for electronic payments for the CCR program and requested technical assistance from DISA.

Effects of Slow Progress of CCR

As a result of slow progress in registering contractors and implementing a fully-functional CCR program, the vision of collecting standardized contractor information in a centralized location to eliminate duplication and inefficiency is not being realized. Also, contractors are not complying with Federal Acquisition Regulation 4.503, Contractor Registration, requirements.

In addition, the ability to use the CCR data for electronic payment and for preparing the required Internal Revenue Service form 1099 is at risk. The recently enacted Debt Collection Improvement Act of 1996, requires Federal Agencies to have the Taxpayer Identification Number of every contractor they do business with and to pay contractors through electronic funds transfer. Sections 6041 and 6041A of title 26, United States Code, require Federal Government agencies, to report certain payments for services to the Internal Revenue Service on Internal Revenue Service Form 1099-Misc, Miscellaneous Income. This requirement for reporting contractor payment information has been incorporated into the FAR and DoD Manual 7220.9-M, DoD Accounting Manual, December 14, 1987.

Corrective Actions Taken by Management

At the conclusion of our audit, we met with the Executive Director, Electronic Commerce Integration Organization, and personnel from DISA to discuss our findings. The Executive Director told us that the Debt Collection Improvement Act of 1996 is expected to have significant impact on the CCR since the Defense Comptroller has declared the CCR as the source of all EFT information for DoD contract payments. The Debt Collection Improvement Act is the driving force behind the restructuring of CCR. In March 1997, the Director, Defense Procurement established an overarching integrated product team to define and prioritize the requirements for CCR to implement the provisions of the Debt Collection Improvement Act. The overarching integrated product team pulled together members from all the DoD agencies and Services affected by the Debt Collection Improvement Act and changes to CCR. Significant progress has been made by the overarching integrated product team since the end of March, resulting in restructuring the processes and management of CCR.

The Executive Director also told us that he had taken several initiatives since March 31, 1997, that would improve progress on the CCR program. Those initiatives included:

CCR Mandate. Members of the overarching integrated product team have worked with the Defense Acquisition Review Council in drafting and coordinating Defense Federal Acquisition Regulation (DFAR) changes to require contractor registration for all vendors, not just EC/EDI vendors doing

Finding A. Progress of the Central Contractor Registration

business with DoD. The proposed DFAR changes support the Director of Defense Procurement memorandum of February 1997. The proposed DFAR changes will be published in the Federal Register for industry comment.⁴

In February 1997, DFAS began stamping the envelopes of vendor check payments and remittance advices with information on the need to register in CCR to continue to receive payments. Procurement offices have also begun to attach a similar notice to solicitations.

Progress of Registration. Prior to March 1997, the average number of CCR vendor registrations per month was approximately 500. April figures show an increase in registrations of over 400 percent per month, while figures extrapolated from the first week of May indicate a 700 percent monthly increase. Although the number of registrations is substantially increasing since the Director, Defense Procurement policy memo and the DFAS and Procurement notices, the number of registrations still falls far short of the estimated 400,000 potential DoD contractors. As a result, the overarching integrated product team was forced to look at alternative methods to populate CCR other than by individual registrations. The overarching integrated product team concluded that a seed file of approximately 300,000 vendors was required.

Use of Existing Data Bases to Populate CCR. The premise of the recommended seed file is to utilize existing government and commercial vendor data bases and batch validations techniques to the maximum extent possible to build a seed file with the maximum number of data elements required to populate CCR. The overarching integrated product team has employed the services of Dunn and Bradstreet and the Defense Manpower Data Center to merge the appropriate data elements from the Federal Procurement Data Center, PASS, CAGE and Dunn and Bradstreet files, along with the already merged DFAS vendor pay and contract files from the Defense Comptroller's Operation Mongoose project. This seed file will consolidate vendor data from many data sources, and in response to the draft report, this seed file is expected to be loaded and verified for accuracy by November 1997.

Promoting the CCR Program. Negotiations are underway with the ECRCs and Procurement Technical Assistance Centers for support and promotion of CCR. It is expected that a written agreement with the ECRCs will be in place soon.

Use of CCR Data for Contracting, Electronic Payment and Tax-Related Information Reporting. The overarching integrated product team has placed the Debt Collection Improvement Act requirements as top priority changes for

⁴ The proposed DFAR changes were submitted to the Federal Register on September 15, 1997 and are being tracked as DFAR Case No. 97-D005.

Finding A. Progress of the Central Contractor Registration

CCR. As a result, several changes in management direction have been made to accommodate the Debt Collection Improvement Act requirements as quickly as possible:

The DoD Comptroller, DFAS and Service and agency financial and contracting officials have fully participated to identify a set of minimum data elements required by their respective communities to utilize CCR data. Registration forms are being simplified to reflect the changes. The identification of this minimum data element set has minimized the impact of registration on the vendor community.

Alternative methods for transmitting required data elements are being investigated. Individual Service and agency meetings are scheduled to work out the most expeditious and cost effective solution for passing data to service and agency legacy automated information systems.

An interactive voice response system is in the planning stages to provide phone query capabilities for those contracting and finance offices with insufficient hardware and software for Web access.

Recommendations, Management Comments, and Audit Response

Revised, Renumbered, Redirected, and Deleted Recommendations. As a result of management comments to our draft report and additional discussions with representatives of the Under Secretary of Defense (Comptroller), we revised Recommendation A.2. and A.3. to exclude the Under Secretary of Defense (Comptroller) from Recommendations A.2. and A.3. In addition, we deleted Recommendation A.6.a. for the Military Traffic Management Command to develop automated systems that will perform the required Internal Revenue Service reporting requirements for the Internal Revenue Service Form-1099, Miscellaneous-Income. Subsequent legal research concluded that freight carriers are exempt from the Internal Revenue Service Code requirements to file Form 1099 with the Internal Revenue Service. As suggested by Military Traffic Management Command in its comments to the draft report, we have redirected Recommendation A.6.c. to the Director, DFAS as Recommendation A.7.

1. We recommend that the Executive Director, Electronic Commerce Integration Organization:

a. Conduct a cost effectiveness study and technical assessment for using existing databases to populate the CCR database.

Finding A. Progress of the Central Contractor Registration

b. Use CD-ROM disks or other appropriate electronic methods to distribute the Central Contractor Registration data to DoD contracting offices and payment offices until all users are provided capability to access the data through FACNET.

Under Secretary of Defense for Acquisition and Technology and Electronic Commerce Integration Organization Comments. The Electronic Commerce Integration Organization concurred with Recommendations A.1.a. and A.1.b. On Recommendation A.1.a., the Electronic Commerce Integration Organization stated that it is in the process of populating the CCR database with contractor information obtained from a Dun and Bradstreet. It expected to complete this project by November 1997. On Recommendation A.1.b., the Electronic Commerce Integration Organization stated that it is reviewing procedures and electronic methods for distribution of CCR data to DoD contracting offices. It expected to have the information in the CCR available to contracting officers by April 1998.

2. We recommend that the Director, Defense Procurement develop an information package on the Central Contractor Registration System and encourage the DoD Small Business Offices, finance offices, and contracting offices to provide the packages to potential contractors.

Director, Defense Procurement Comments. The Director, Defense Procurement concurred with the recommendation. The Director, Defense Procurement stated that she will, in coordination with Deputy Under Secretary of Defense (Logistics), Electronic Commerce Integration Organization, develop an information package on the CCR by December 1997.

3. We recommend that the Director, Defense Procurement:

a. Direct the Services' Senior Acquisition Executives to upgrade the computer equipment and software used by their respective contracting officers so that those users can access and use the Central Contractor Registration database.

b. Require that all DoD contracting officers be trained to access and use the Central Contractor Registration database.

c. Publish information on the requirement to register for the Central Contractor Registration in the Commerce Business Daily.

Director, Defense Procurement Comments. The Director, Defense Procurement concurred with Recommendations A.3.a., A.3.b., and A.3.c. On Recommendation A.3.a. the Director, Defense Procurement stated that the CCR Integrated Product Team created by Director, Defense Procurement will work with the Military Departments, Defense agencies, and the Defense Finance and Accounting Service to ensure those organizations are able to access the CCR database. Direction has already been provided to the Military departments to upgrade their computer systems. On Recommendation A.3.b., Director, Defense Procurement stated that an information package discussed in

Finding A. Progress of the Central Contractor Registration

Recommendation A.2. will include a section on training for DoD contracting officers. On Recommendation A.3.c., the Director, Defense Procurement stated that she will publish the requirement for contractors to register in the CCR as a proposed Defense Federal Acquisition Regulation supplement rule in the Federal Register rather than in the Commerce Business Daily.

4. We recommend that the Director, Defense Finance and Accounting Services establish the necessary interfaces in its automated systems to use the Central Contractor Registration data for Internal Revenue Service Form 1099 generation and electronic payment of funds to DoD contractors.

Defense Finance and Accounting Service Comments. Comments were not received.

Audit Response. We request that the Defense Finance and Accounting Service respond to Recommendation A.4. by November 24, 1997.

5. We recommend that the Executive Director, Electronic Commerce Integration Organization develop training courses on access and use of the Central Contractor Registration database.

Under Secretary of Defense for Acquisition and Technology, Electronic Commerce Integration Organization Comments. The Director, Electronic Commerce Integration Organization concurred. The Electronic Commerce Integration Organization stated that it intended to develop a CCR access and usage guide to facilitate contracting officer awareness and knowledge of CCR. The Electronic Commerce Integration Organization expects to develop this guide and distribute it to DoD contracting officers by April 1998.

6. We recommend that the Commander, Military Traffic Management Command require its personal property carriers and freight carriers to register in the Central Contractor Registration database.

Military Traffic Management Command Comments. Military Traffic Management Command concurred with the recommendation. The Military Traffic Management Command stated that it had been actively working to assure that freight and personnel carriers are made aware of and provide information needed by CCR database. On June 11, 1997, the Under Secretary of Defense (Comptroller) and the Director, Defense Procurement issued a memorandum announcing that the deadline for registering for the CCR had been moved from September 30, 1997 to March 31, 1998. Military Traffic Management Command stated that they would work with the guidance of this memorandum to populate the database.

7. We recommend that the Director, Defense Finance and Accounting Service establish procedures for prepare the DD Form 350, Individual Contracting Action Report, for all personal property carriers and freight carrier transactions that are expected to cost \$25,000 or more so that those transactions are properly reported to the Internal Revenue Service as required by the Internal Revenue Code, Section 6050M.

Finding A. Progress of the Central Contractor Registration

Audit Response. We request comments from the Director, Defense Finance and Accounting Service on Recommendation A.7. by November 24, 1997.

Finding B. CCR Data Access Protection

Although DISA has significantly improved security of the CCR and protection of the CCR data, additional security improvements are needed to:

- Ensure that the CCR can comply with Controlled Access Protection level C2 security requirements.
- Protect the CCR from unauthorized access.
- Protect CCR data submitted over the Internet.

Without these additional protections provided by Controlled Access Protection level C2 compliant systems, additional firewalls, and a secure Internet web server, CCR data will be subject to increased risk of improper access or disclosure of sensitive information.

Data Access Protection Policy and Security Standards

Need for Security. The CCR must protect registered contractors from financial harm as a result of unauthorized access or disclosure of sensitive information submitted for registration. Data submitted includes taxpayer identification numbers, bank account information and Electronic Funds Transfer routing information. DoD contracting officers have a responsibility to protect such data from disclosure and to protect its integrity from unauthorized access.

Data Access Policy. DoD Directive 5200.28, Security Requirements for Automated Information Systems, March 21, 1988, requires automated information systems to have class C2 protection if the system processes sensitive, unclassified information. Class C2 requires controlled-access protection to prevent unauthorized users from reading and modifying sensitive information on the network. Controlled access protection can be accomplished by providing identification and authentication, discretionary access control, audit, and object re-use capabilities.

Identification and authentication of users ensure that the user is authorized to access the system, and users are who they claim to be. Discretionary access control limits users' access to system resources according to the access level that they are authorized to accomplish their work. Auditing tracks user accesses, tracks problems that arise, and makes tools available for detecting when unauthorized accesses are attempted or succeed. Object re-use is essentially the clearing of either computer or disk memory between tasks to reduce the

Finding B. CCR Access Protection

potential that subsequent lower-access tasks or users do not gain inadvertent access to higher-access information by re-using the same memory or disk space.

Security Standards. The American National Standards Institute established a standard, standard X12.58, Security Structures, for data authentication and encryption. The standard is intended to verify the identity of the sender for the recipient of the transaction; verify the data integrity; provide confidentiality of the business data; and detect insertions, modification, deletion, or impersonation.

Prior FACNET Security Audit

Inspector General, DoD, Report No. 96-214, Computer Security for the Federal Acquisition Computer Network, was issued on August 22, 1996. The report recommended that DISA enhance network security by implementing a firewall protection mechanism, by establishing digital data encryption and authentication capabilities, and by ensuring that FACNET complies with C2-level controlled-access protection requirements. Since that audit, DISA has made significant improvements in security over the FACNET system; and the security personnel that we talked to were both knowledgeable and dedicated to improving security for the system. Specifically, DISA has implemented the report recommendations by installing firewalls at DISA gateways, by using digital data authentication and encryption technology in the CCR transactions that are submitted via an Internet Web-based server, and by upgrading most of its operating systems to comply with C2 level controlled-access protection requirements.

Class C2 Level Security Requirements

FACNET and the CCR have been designated as containing sensitive, but unclassified information (that is, bank account numbers, taxpayer identification numbers). DoD Directive 5200.28 requires such systems to meet the C2 level security requirements. To meet those requirements, the operating system used on all the computers must provide controlled access protection to prevent unauthorized users from reading and modifying sensitive information on the network. At the time of our visit, DISA had installed operating systems that conform to the C2 level requirements at all of its Electronic Commerce Processing Nodes (ECPNs) and on the CCR Interface computer but had not yet installed an approved operating system on its CCR computer. Instead, the CCR computer was using an older version of the Hewlett Packard operating system

that does not satisfy the C2 level security requirements. DISA needs to upgrade the operating system to HP-UX version 10 (or later) to satisfy the C2 level security requirements.

Firewall Protection of CCR Data

DISA had installed firewall protection capabilities at the DISA Megacenters Columbus and its Megacenters Ogden. Both Megacenters host ECPNs for FACNET, and the Megacenters Columbus is the host site for the CCR data. Both locations are using a commercial firewall package known as CheckPoint. The firewall is intended to restrict network access to authorized users and can be programmed by computer security personnel to restrict access to certain sites, or certain users. The firewalls, as installed by DISA, provide an added layer of security protection to its network, but, because it is installed at the Megacenters level rather than at the application level, it cannot restrict access to CCR-authorized users. The CCR data access controls can be significantly enhanced by installing an additional firewall, specifically for the CCR program, that will limit access to authorized VANs and gateways.

Secure Internet Web Server Capability

Since October 1996, DISA has made an Internet web server available as one way for contractors to register with the CCR. This capability can encourage additional contractors to register for the CCR. As of March 31, 1997, there were 583 contractors that had registered through this web server. Although sending information over the Internet entails some risk, information that is encrypted in a manner that meets or exceeds the existing standards for encryption, and uses digital signatures to authenticate the user, can be used to communicate sensitive transactions in a secure manner. In fact, commercial banks have begun to use the Internet for bank transactions⁵.

DISA has implemented a commercial application that authenticates users by using digital data encryption. This application, called VeriSign, can be optionally used by a contractor submitting registration information over the Internet, to authenticate CCR registration data and to ensure that data has not been altered in

⁵The Security First Network Bank, Atlanta, Georgia, is a Federal Deposit Insurance Corporation insured bank that does banking exclusively over the Internet. Other, more traditional banks, such as Chase Manhattan, have announced that they are also exploring the Internet as a possible method of conducting transactions.

Finding B. CCR Access Protection

route to the server. VeriSign encryption technology provides positive identification of the site that submitted the transaction. Digital authentication ensures that data received from trading partners has arrived unaltered. Digital certificates are used to verify each contractor's identification and information content. A digital certificate is a password-protected, encrypted data file that includes:

- the name of the holder and other authentication information, such as email address;
- a public key⁶ which can be used to verify the digital signature of a message sender previously signed with the matching, mathematically-unique, private key; and
- the name of the issuer.

VeriSign, however, only proves identity and precludes transaction alteration while the data is enroute; it does not encrypt the data to protect it from disclosure. Because of the sensitivity of the registration data, we believe DISA should install software on its Internet web server that would protect the data. The most common method of protecting such data is to use software that implements the Secure Sockets Layer (SSL) methodology. SSL works by using a secure socket or port for transferring the information between the server and the client. SSL can also be used for communications such as file transfer protocol. SSL sits between the web browser and the http program on the web server. All information that flows in and out of this secure socket is encrypted and is checked to ensure the information has not been changed enroute.

CCR Data Exposure to Public

CCR data, though unclassified, are considered sensitive because they contain sensitive financial data and other proprietary data which must be protected from dissemination. Of the 60 data elements in the CCR database, 18 are considered sensitive and conditionally releasable. Eight other data elements in the CCR database require strict access control and are not releasable. Because CCR data are vulnerable to unauthorized access, DISA should upgrade the operating

⁶Public-key cryptography enables a user to produce a digital signature by encrypting a document with a private key (password known only to that user), which, when decrypted with that user's public key (which requires no password), provides verification that the document originated from that user.

system to comply with C2 controlled access protection requirements, improve its firewall protections of the CCR program, and install a secure server capability as soon as practical.

Corrective Actions Taken by Management

At the conclusion of our audit, we met with the Executive Director, Electronic Commerce Integration Organization, and personnel from DISA to discuss our findings. The Executive Director told us that Service and agency functional representatives and DISA operations and security personnel had developed a functional risk assessment plan during the week of May 6, 1997. This plan identified security risks, actions to mitigate those risks and the organization responsible to implement the actions. Many of the security risks were based on inadequate definitions of the access and protection requirements for CCR data elements. As a result, the overarching integrated product team members have been tasked to review the data elements and the access and protection required. Sensitive data elements will require documented justification for release. These access requirements are stricter than those currently in place, and appropriate measures will be developed to ensure stricter protections. The revised matrix of data elements is being developed.

The functional risk assessment plan identified other measures of protection that are planned for implementation before the end of June 1997:

- The CCR operating system is scheduled to be upgraded to C2-level compliance.
- Firewalls and transmission control protocol wrappers have been put in place to limit access to CCR.
- Promotion of the secure Internet capabilities has resulted in increased use by individual registrants.

The above actions are a result of management direction to speed the process of populating the CCR, operating the CCR and providing access to the CCR for the contracting and finance officials in order to minimize the risk to the overall CCR program. Cooperation of the Service, agency, and OSD functional representatives was key to the success of initiating the course corrections.

Recommendations, Management Comments, and Audit Response

We recommend that the Director, Defense Information Systems Agency:

- 1. Upgrade the operating system used for its Central Contractor Registration Program, to a version that complies with security requirements for C2-level security.**
- 2. Install a firewall that will restrict access to the Central Contractor Registration Interface computer, Megacentr Columbus, to authorized Value-Added Networks and gateways.**
- 3. Install security software for its Internet web server that will encrypt registration data submitted by its contractors while it is enroute to the server.**

DISA Comments. DISA concurred with Recommendations B.1. and B.3., and concurred in part with Recommendation B.2. On Recommendation B.1., DISA stated that the operating system used for CCR was upgraded to a C2-level security system on July 20, 1997.

On Recommendation B.2., DISA stated that there are two CCR machines commonly referred to as CCR and CCRI. The CCRI machine is separated from the Electronic Center Processing Node and is, in fact, the firewall for the CCR machine. The CCR and CCRI physically reside in the Defense Megacentr Columbus, but there is no physical connection between these two machines. Public procurement officials can access pertinent information in only the CCRI, and to ensure this data is protected, software has been installed to limit the particular view of the data by utilizing user ID/passwords assigned to users. The user ID and password function is performed and controlled by the Defense Logistics Service Center under a customer support agreement. To safeguard the data from hackers, this query capability is directed to a copy of the master database. This copy resides on the CCRI machine, again, used as a firewall for the protection of the CCR master database.

On Recommendation B.3., DISA stated that it is currently using VeriSign encryption technology to provide positive identification of the site submitting the data.

Audit Response. We agree that VeriSign enhances CCR network security by providing positive identification of the site using an encrypted security certificate; and VeriSign can be used to detect any changes to the data while it is enroute to the CCR. However, VeriSign does not encrypt the actual data that it accompanies. Because the actual data is not encrypted, sensitive data submitted during the registration process could be compromised while those transactions

Finding B. CCR Access Protection

are enroute. For this reason, we believe that a secure server, in addition to VeriSign, could provide a high level of security and promote user confidence in CCR.

THIS PAGE INTENTIONALLY LEFT BLANK

Part II - Additional Information

Appendix A. Audit Process

Scope

Audit Work Performed. We determined the progress in registering contractors by examining registration statistics for the period 1994-1997 and comparing that information to estimates of the total number of Government contractors. We compared data elements required for the CCR and compared those elements to data elements in other existing commercial and Government-owned databases. We visited the DLSC and reviewed the process for verification of the CAGE codes. We visited DFAS to access potential users of CCR data for electronic payments by that agency, and assessed DFAS ability to use the data for electronic payment of contractors and Internal Revenue Service reporting. We met with program managers for the Central Contractor Registration Program, and the Director, DoD Electronic Commerce. We contacted DoD Small and Disadvantaged Business Utilization Offices and contracting offices to determine if they were adequately promoting the CCR program to potential and existing contractors. We visited the Small Business Administration to obtain information on the PASS database. We examined selected security controls for the Central Contractor Registration program at the DISA Megacenters, Columbus, Ohio and the Air Force Standard System Group, Maxwell AFB, Montgomery, Alabama, to determine if the sensitive data collected for the system was secure, could be reconstructed in the event of a disaster, and whether the infrastructure for the system met the requirements for C2-level security. Because contractors could also register for the system through a web page on the Internet, we examined security controls for the Internet web server. We interviewed computer security experts and reviewed security requirements promulgated by DoD Directive 5200.28, the American National Standards Institute X.12.58, Security Structures, and contacted various vendors for information on security features of software used by DISA.

Audit Period, Standards, and Locations. We performed this program audit from July 1996 through May 1997. The audit was performed in accordance with auditing standards issued by the Comptroller General of the United States as implemented by the Inspector General, DoD. We did not use statistical sampling procedures in performance of the audit. We relied upon information on the number of records and data elements from the respective data managers for the PASS, DUNS, CAGE, and DD 350 databases; but we did not test the data for accuracy because the estimates provided by the data managers were sufficient to support audit conclusions regarding potential usefulness of the data as a seed file.

Management Control Program

DoD Directive 5010.38, Management Control Program, August 26, 1996, requires DoD organizations to implement a comprehensive system of management controls that provides reasonable assurance that programs are operating as intended and to evaluate the adequacy of the controls.

Scope of Review of the Management Control Program. We reviewed the adequacy of DISA management controls over the CCR as they pertain to the progress of program implementation and access controls over sensitive contractor information contained in the program's database. Because we did not identify a material weakness, we did not assess management's self-evaluation.

Adequacy of Management Controls. DISA management controls over the CCR were adequate as they applied to the audit objectives.

Appendix B. Summary of Prior Audits and Other Reviews

Two General Accounting Office reports pertain to the CCR and security issues of FACNET. The Inspector General, DoD, has issued other reports relating to the EC/EDI program and one report on Internal Revenue Service reporting for contractor payments. Additionally, the Office of Management and Budget has issued a report on Federal agency tax-related information reporting.

General Accounting Office

GAO/NSIAD-97-26, Acquisition Reform Obstacles to Implementing the Federal Acquisition Computer Network, January 3, 1997, states that effective implementation of the CCR database is fundamental to current FACNET strategy and achieving a single face to industry. The database has been experiencing significant problems, is far behind schedule, and is still not performing its intended role of operating as the single Federal contractor registration program. As a result, agencies must award contracts to unregistered vendors because the CCR database does not have sufficient registered vendors to supply the full range of products and services needed. In fact, 16 of the 17 agencies contacted reported the lack of a well-populated and operational CCR database as a great or very great obstacle to efficient and effective implementation of FACNET. The report recommended that the Director, Office of Management and Budget, ensure the Administrator for Federal Procurement Policy in consultation with the Department of Defense and other agencies, develop a strategy to implement electronic commerce technologies including the FACNET. National Aeronautics and Space Administration, General Services Administration, Office of Federal Procurement Policy, and DoD generally agreed with the findings and recommendations.

GAO/T-NSIAD/AIMD-95-190, Implementation of the Federal Acquisition Streamlining Act of 1994, July 20, 1995, reported that Government-wide standards for protecting the security of sensitive procurement information were not yet defined. The report made no recommendations.

Inspector General, DoD

The Inspector General, DoD, has issued the following reports that specifically pertain to EC/EDI and Internal Revenue Service reporting requirements.

Inspector General, DoD, Report No. 97-103, Summary Report on the DoD Implementation of Electronic Commerce/Electronic Data Interchange in Contracting for Small Purchases and the Federal Acquisition Computer Network, March 4, 1997. The report found that despite intensive efforts, DoD has experienced delays in the successful implementation of FACNET for small purchases and significant issues still need to be resolved. The report recommended that the Deputy Under Secretary of Defense (Logistics) perform an analysis of FACNET and alternative electronic commerce vehicles and identify how and when each electronic commerce vehicle should be used. The Director, DoD Electronic Commerce, nonconcurred with the report recommendations. The report has been forwarded to Audit Followup.

Inspector General, DoD, Report No. 97-090, Electronic Commerce Resource Centers, February 11, 1997. The report found that the Electronic Commerce Resource Centers (ECRC) have not been efficient or cost effective in promoting the implementation or increased use of EC/EDI technologies between Government organizations and vendors. As a result, DoD obligated approximately \$81.5 million for FY 1994 through the first quarter of FY 1996 that did not greatly increase the implementation and use of EC/EDI technologies. The report recommended that the Deputy Under Secretary of Defense (Logistics) seek additional time to implement the congressional direction to establish five new ECRC sites. The report also recommended that the Deputy Under Secretary of Defense (Logistics) streamline the multi-layered ECRC management structure; redirect the ECRC program with focus on getting DoD procurement offices and vendors to use EC/EDI technologies; establish contractor performance measures; establish a Government-wide EC/EDI integrated process team to optimize collaborative efforts; coordinate ECRC efforts with Defense Logistics Agency managed Procurement Technical Assistance Center efforts; and seek authorization to eliminate the congressionally-directed ECRC technology hub. The Deputy Under Secretary of Defense (Logistics) concurred with and are implementing most of the recommendations in the report. The Under Secretary of Defense (Logistics) and the Defense Logistics Agency non-concurred with the recommendation on the technology hub.

Inspector General, DoD, Report No. 97-030, DoD Interim Federal Acquisition Computer Network Certification, November 25, 1996. The report found that 5 of the 13 contracting offices reviewed were interim FACNET certified, but were not capable of meeting prescribed requirements for interim FACNET certification. As a result, the contracting offices were not capable of sending and receiving FACNET transactions, and contracting offices and their trading partners may be affected by potential loss of business. The report recommended

Appendix B. Summary of Prior Audits and Other Reviews

that the Deputy Under Secretary of Defense (Acquisition Reform), revise the process for interim FACNET certification to require that the Defense Information Systems, working in conjunction with the Military Departments and Defense agencies, conduct technical compliance testing at each contracting office seeking certification, and conduct technical compliance testing again at the contracting offices previously certified. The Defense Information Systems Agency partially concurred with the findings and recommendations. DISA fully agreed that some type of testing is required before an automated information system is declared operational.

Inspector General, DoD, Report No. 97-010, Defense Information Systems Agency Management of Trouble Tickets for Electronic Commerce/Electronic Data Interchange, October 28, 1996. The report found that the Defense Information Systems Agency has not resolved recurring problems identified by the trouble ticket process. The recurring problems identified were invalid transactions, lost and late transactions, inability to track transactions, and lack of acknowledgments for receipt of transaction. The report recommended that the Director, Defense Information Systems Agency establish milestones for redesign of the FACNET infrastructure to promptly resolve the recurring problems identified in this report. Moreover, until the redesign is complete, they should implement interim procedures to correct recurring problems. The Director, Defense Information Systems Agency, concurred with the report recommendations.

Inspector General, DoD, Report No. 97-002, Vendor Participation in the Federal Acquisition Computer Network, October 4, 1996. The report found that out of 100 vendors surveyed, 85 identified 3 major impediments to using the Federal Acquisition Computer Network. As a result, DoD was losing credibility with vendors regarding development and implementation of the Federal Acquisition Computer Network. The report recommended that the Deputy Under Secretary of Defense (Acquisition Reform):

- define when use of the Federal Acquisition Computer Network is appropriate and require contracting officials to use it accordingly;
- identify and implement an effective method for disseminating information about the Federal Acquisition Computer Network;
- fund only those outreach methods that are deemed effective, and
- require contracting officials to reference optional Federal Acquisition Regulation clauses rather than provide the full text.

The report also recommended that the Director, Defense Information Systems Agency verify that implementation of the Electronic Commerce Processing Node (new infrastructure) corrects technical problems associated with the Federal Acquisition Computer Network. In addition, the report recommended that the Director identify interim measures and corrective actions for resolving technical problems identified in this report, until implementation of the

Appendix B. Summary of Prior Audits and Other Reviews

Electronic Commerce Processing Node is implemented. The Deputy Under Secretary of Defense (Acquisition Reform) and the Defense Information Systems Agency concurred with the report recommendations.

Inspector General, DoD, Report No. 96-214, Audit of Computer Security For The Federal Acquisition Computer Network, August 22, 1996. The report found that the Defense Information Systems Agency had not obtained capabilities for digital signatures or encryption for procurement transactions sent over FACNET. As a result, FACNET transactions could suffer undetected alterations, may not satisfy legal requirements and may be subject to compromise. The Defense Information Systems Agency had not established data backup procedures or developed the required continuity of operations plans for FACNET. As a result, the ability of FACNET to recover operations following a disaster is not assured. The Defense Information Systems Agency, Electronic Commerce and Electronic Data Interchange Program Management Office had not provided adequate controlled access protection for FACNET. As a result, FACNET is not protected from fraud and criminal threats. The report recommended that the Deputy Under Secretary of Defense (Acquisition Reform) approve a plan and establish milestones for implementing digital signatures and data encryption for the FACNET system, and limit use of FACNET transactions that require signatures until the Defense Information Systems Agency obtains digital signature capabilities. The report recommended that the Director, Defense Information Systems Agency develop backup procedures for FACNET gateways that include storage of critical data at an off-site location; and develop continuity-of-operations plans for the gateways. The report recommended that the Defense Information Systems Agency, Electronic Commerce and Electronic Data Interchange Program Management Office enhance network security by implementing a firewall protection mechanism and by ensuring that FACNET complies with controlled access protection requirements. The Director, Defense Information Systems Agency, concurred with the report recommendations.

Inspector General, DoD, Report No. 96-172, Audit of Certification Management of Value-Added Networks, June 21, 1996. The report found that the Defense Information Systems Agency did not establish an adequate Government VAN certification process and did not adequately monitor VANs for compliance with the VAN License Agreement. This report recommended that the Director, Defense Information Systems Agency issue policy requiring enforcement of compliance with the Federal Acquisition Regulation 9.104, Contractor Qualifications, to include establishing a system for evaluating business qualifications such as a weighted procedure or point system; issue policy for monitoring VANs for compliance with the VAN License Agreement; and expedite the completion and issuance of the new VAN License Agreement. DISA partially concurred with the report recommendations.

Inspector General, DoD, Report No. 96-129, Review of DoD Implementation of Electronic Commerce in Contracting for Small Purchases, May 24, 1996. This report identified and summarized issues related to the implementation of

Appendix B. Summary of Prior Audits and Other Reviews

electronic commerce within DoD. This report contained no findings or recommendations, comments were not required, and none were received.

Inspector General, DoD, Report No. 96-057, Audit of DoD use of Electronic Bulletin Boards in Contracting, January 8, 1996. The DoD procurement offices did not use bulletin boards to circumvent or impede FACNET implementation. Rather, procurement officials were using bulletin boards as an interim means to meet their procurement requirements until the Government-wide FACNET is fully operational. Also, procurement officials were not investing significant resources to establish new bulletin boards or to upgrade existing capabilities because officials were committed to phasing out their use of bulletin boards once FACNET becomes fully operational. Although not required to comment, the Deputy Assistant Secretary of the Air Force (Contracting), Office of the Assistant Secretary of the Air Force (Acquisition), provided comments to the draft audit report. The Deputy Assistant Secretary concurred with the audit results and emphasized the need for a commonly accepted set of goals and definitions to be used in implementing electronic commerce/electronic data interchange.

Inspector General, DoD, Report No. 95-234, DoD Compliance with Federal Tax Reporting Requirements, June 14, 1995. The Report found that overall DoD management of the Internal Revenue Service Form 1099 reporting process was inadequate. Specifically, 10 of the 11 DoD paying offices visited were not obtaining needed information, maintaining accurate records, or reporting payments for noncorporate contractors and certain medical service corporations. These conditions existed because DoD contracting offices did not always provide DoD Paying Offices the taxpayer information needed to perform Internal Revenue Service Form 1099 reporting. The report recommended that the Under Secretary of Defense for Acquisition and Technology enforce compliance with the FAR 52.204-3 and 4.203, which require contracting officers to obtain taxpayer identification numbers, corporate status, and contract type for all procurement actions, regardless of dollar value; and submit the information to the paying office. The management concurred and stated that DoD was already complying with taxpayer reporting requirements that apply to actions in excess of \$25,000, via implementation of FAR 4.903. For actions below \$25,000, the DoD proposed to achieve compliance with FAR 52.204-3 and 4.203 requirements via the registration of all vendors that do business with DoD in CCR. The management comments anticipated that CCR will be substantially complete within 2 years.

Office of Management and Budget

Office of Management and Budget Report to Congress, Improvements Needed in Federal Agency Tax-Related Information Reporting to Ensure Tax Compliance of Federal Contractors, April 1, 1994, concluded that Federal

Appendix B. Summary of Prior Audits and Other Reviews

agencies were not complying with Internal Revenue Service Form 1099 reporting requirements, and that 22 percent of contractors doing business with the Government owed delinquent taxes. The report recommended that Federal agencies take immediate steps to check contractors' tax compliance; that Federal agencies certify that procedures and policies are in place by March 30, 1995, to meet Internal Revenue Service Form 1099 reporting requirements; and that Federal agencies and the Internal Revenue Service ensure that the required taxpayer identification numbers are obtained and verified.

Appendix C. Summary of Data Elements

Description	CCR	DUNS	TIN	PASS	CAGE	SF129	DD 350
Accounting closing period	X						
Acceptance federal electronic instruction	X						
Administrative contact	X			X			
Affiliate name	X			X	X	X	
Affiliated company DUNS	X						
Applicant's additional name information	X		X		X		
Applicant's name	X		X		X		
Applicant's Taxpayer Identifying Number (TIN)	X		X	X	X		X
Applicant's trading partner identification number	X						
Authorized financial contact	X						
Bank routing transit number	X						
Business address	X	X	X	X	X	X	X
Business name (legal name)	X	X	X	X	X	X	X
Business ownership	X			X		X	
Certification of application information	X		X	X		X	
Commercial and Government Entity (CAGE)	X			X	X		X
Contract administrative office	X				X		
Currency for payment	X						
Data Universal Numbering System Number	X			X	X	X	
Date business started or acquired	X	X		X		X	
Date of application	X			X	X	X	
EDI capabilities transaction, versions and release	X						

Key to Data Elements

CCR: Central Contractor Registration data elements

DUNS: Data Universal Numbering System data elements

TIN: Taxpayer Identification Number data elements

PASS: Procurement Automated Source System data elements

CAGE: Commercial and Government Entity data elements

SF129: Solicitation Mailing List Application data elements

DD 350: Individual Contracting Action Report data elements

Appendix C. Summary of Data Elements

Description	CCR	DUNS	TIN	PASS	CAGE	SF129	DD 350
EDI coordinator name, phone, fax, e-mail	X						
Facility security clearance	X			X		X	
Financial institution address	X						
Financial institution telephone and contact person	X						
Gateway provider	X						
Geographic locations company wants business in	X			X			
Government purchase card	X			X			
Highest employee security clearance	X			X			
Equipment, supplies, services offered	X					X	X
If checks are preferred, remittance address	X						
If minority owned, is it 8(a) certified firm	X			X	X		X
Interfaces with Automated Information Systems	X						
Machine to machine communications number	X						
Manufacturing quality assurance	X			X			
Name of bank where payment is sent	X						
Name of county	X				X		
Network Entry Point	X						
Parent company name	X			X	X	X	X
Party authorized to sign legal documents	X						X
Party submitting quotes	X						
Party to perform packaging	X						
Party to receive electronic remittance advice	X						
Party to receive purchase orders	X						
Party to receive solicitations	X						
Point of contact for information	X						
Registering party-average no. of employees	X						X
Registrant business	X						
Registrant authorized financial name, phone	X						
SBA certified 8a firms only	X						
Standard Industrial Classification (SIC)	X			X	X		X
Tax reference/tax exempt organization	X						
Three-year average revenues	X						X
Translation software provider	X						
Type of application	X		X	X	X	X	X
Type of business	X			X	X	X	X
Type of organization	X	X	X	X	X	X	
Vendor's bank account title and number	X						
Vendor's preferred method of payment	X						

Key to Data Elements

CCR: Central Contractor Registration data elements

DUNS: Data Universal Numbering System data elements

TIN: Taxpayer Identification Number data elements

PASS: Procurement Automated Source System data elements

CAGE: Commercial and Government Entity data elements

SF129: Solicitation Mailing List Application data elements

DD 350: Individual Contracting Action Report data elements

Appendix D. Glossary

Digital Signature. Transformation of a message using cryptography so the author of a document can be positively identified and any alteration of that document can be readily detected.

Electronic Commerce. End-to-end, paperless business environment that integrates electronic transfer and automated business systems.

Electronic Commerce Processing Node (ECPN). FACNET computers used to connect the gateways to the value added networks. FACNET network entry points are used to control the flow and routing of procurement transactions through the network. The two FACNET ECPNs are located in Ogden, Utah, and Columbus, Ohio.

Electronic Data Interchange. Exchange of information without human intervention, using a standardized format.

Encryption. The process to transform plaintext into ciphertext or enciphered data to prevent disclosure of the information.

Firewall. A type of router that is placed between a network and the Internet to filter incoming and outgoing traffic to enhance network security.

Gateway. A device for hardware or software that converts one network's message protocol to format used by another network. Used to connect the Government's procurement offices to the network.

Internet. The inter-connection of existing corporate and Government networks using commonly used telecommunications standards; collection for networks and gateways that use the Transmission Control Protocol/Internet Protocol (TCP/IP) suite.

Internet Web Browser. A browser is an application that knows how to interpret and display documents that it finds on the World Wide Web.

Secure Sockets Layer (SSL). An Internet security technique that ensures that all data flowing between a user's computer and a web server is encrypted and has not been changed enroute.

Value-Added Network. A commercial communications network that supplies communication services, usually in the form of store and forward capability, to multiple users for transmitting information. Also provides application services (that is, electronic-mail) and related administrative services.

Web Server. A resource available on the Internet which provides a graphical interface to users who wish to use Internet services.

Appendix E. Report Distribution

Office of the Secretary of Defense

Under Secretary of Defense for Acquisition and Technology
Deputy Under Secretary of Defense (Acquisition Reform)
Deputy Under Secretary of Defense (Logistics)
Executive Director, Electronic Commerce Integration Organization
Director, Defense Logistics Studies Information Exchange
Director, Defense Procurement
Under Secretary of Defense (Comptroller)
Deputy Chief Financial Officer
Deputy Comptroller (Program/Budget)
Assistant Secretary of Defense (Command, Control, Communications, and Intelligence)
Assistant Secretary of Defense (Public Affairs)

Department of the Army

Auditor General, Department of the Army

Department of the Navy

Assistant Secretary of the Navy (Financial Management and Comptroller)
Auditor General, Department of the Navy

Department of the Air Force

Assistant Secretary of the Air Force (Financial Management and Comptroller)
Auditor General, Department of the Air Force

Other Defense Organizations

Director, Defense Contract Audit Agency
Director, Defense Finance and Accounting Service
Director, Defense Information Systems Agency
Director, Defense Logistics Agency
Director, Defense Logistics Services Center

Other Defense Organizations (cont'd)

Director, National Security Agency
Inspector General, National Security Agency
Commander, U.S. Transportation Command

Non-Defense Federal Organizations

Financial Implementation Team for Electronic Commerce, Chief Financial Office
Electronic Commerce Task Force, CFO Council
General Services Administration, Federal Electronic Commerce Acquisition Program
Management Office
Internal Revenue Service, Office of Payer Compliance
National Institute of Standards and Technology, Federal Electronic Data Interchange
Secretariat
Office of Management and Budget, Office of Federal Procurement Policy
Small Business Administration
Technical Information Center, National Security and International Affairs Division,
General Accounting Office

Chairman and ranking minority member of each of the following congressional committees
and subcommittees:

Senate Committee on Appropriations
Senate Subcommittee on Defense, Committee on Appropriations
Senate Committee on Armed Services
Senate Subcommittee on Acquisition and Technology, Committee on Armed
Services
Senate Committee on Governmental Affairs
House Committee on Appropriations
House Subcommittee on National Security, Committee on Appropriations
House Committee on National Security
House Subcommittee on Military Procurement, Committee on National Security
House Committee on Government Reform and Oversight
House Subcommittee on National Security, International Affairs, and Criminal
Justice, Committee on Government Reform and Oversight
House Committee on National Security

THIS PAGE INTENTIONALLY LEFT BLANK

Part III - Management Comments

Under Secretary of Defense for Acquisition and Technology Comments



ACQUISITION AND
TECHNOLOGY

OFFICE OF THE UNDER SECRETARY OF DEFENSE

3000 DEFENSE PENTAGON
WASHINGTON, DC 20301-3000

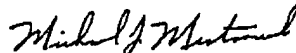
15 JUL 1997.

MEMORANDUM FOR INSPECTOR GENERAL, DEPARTMENT OF DEFENSE
ATTN: Director, Contract Management

SUBJECT: Draft Audit Report on Federal Acquisition Computer Network Central Contractor
Registration Program (Project No. 6CA-0070)

REFERENCE: DODIG Report, subject as above, 10 Jun 97

The Electronic Commerce Integration Organization (ECIO) has reviewed the subject draft report. Our detailed management comments are enclosed. The point of contact for this action is Major Paul Yandik at (703) 696-0419.


Michael J. Mestrovich, Ph.D.
Executive Director, Electronic Commerce
Integration Organization

Attachment



COMMENTS TO DODIG DRAFT AUDIT REPORT ON
FEDERAL ACQUISITION COMPUTER NETWORK CENTRAL
CONTRACTOR REGISTRATION PROGRAM
(Project No. 6CA-0070)

1. GENERAL REPORT COMMENTS: In general, we concur with the draft report. However, the following comments should be considered for incorporation into the final report:

a. On page 2, the draft report incorrectly states that the Federal Acquisition Reform Act of 1996 eliminated the requirement for individual Government contracting offices to become interim FACNET certified. The Federal Acquisition Reform Act of 1996 deleted the requirement for attaining interim FACNET certification before simplified acquisition procedures could be used between \$50,000 and \$100,000. The effect of this change allowed all contracting officers to take advantage of the increased simplified acquisition threshold. However, in accordance with the Federal Acquisition Regulation (FAR), any contracting activity wanting to engage in Electronic Commerce is still required to become interim FACNET certified pursuant to FAR 4.505.

Revised

b. Throughout the draft report, the number of contractors registered in CCR is given as 6,483. Although well below the target number of potential Government contractors, the number of contractors registered in CCR has increased significantly since the draft report was published. As of July 3, 1997, there were 11,678 contractors registered in the CCR database.

Revised

c. The CCR registration mandate (referenced on pages 10 and 11 of the draft report), requiring all contractors to be registered in the CCR database by September 30, 1997, has been superseded. On June 11, 1997, a joint CCR policy letter signed by the Director, Defense Procurement and the Defense Department Comptroller extended the deadline for CCR registration to "no earlier than March 31, 1998."

Page 9
Revised

2. RECOMMENDATION 1.a: Conduct a cost effectiveness study and technical assessment for using existing databases to populate the CCR database.

RESPONSE: We are in the process of populating the CCR database with contractor information obtained from a Dun and Bradstreet "seed file" using files as described on page 23 of the report in the paragraph entitled "Use of Existing data bases to Populate CCR." After loading information from this seed file into CCR, we will be contacting these "new registrants" to ensure the seeded information is accurate and to fill in remaining CCR data elements. We expect to complete this project by November 1997. We expect this effort to substantially increase the number of registrants in CCR, to nearly 300,000.

Revised

3. RECOMMENDATION 1.b: Use CD-ROM disks or other appropriate electronic methods to distribute the Central Contractor Registration data to DoD contracting offices and payment offices until all users are provided capability to access the data through FACNET.

RESPONSE: Concur. We are currently reviewing procedures and electronic methods for distribution of CCR data to DoD contracting offices. The frequency and format for this CCR database distribution are currently being defined with the cooperation of the military services and agencies. We expect to have the information in the CCR available to contracting officers as required by the CCR Policy memo referred to in paragraph 1c. above by April 1998.

4. RECOMMENDATION 5: Develop training courses on access and use of the Central Contractor Registration database.

RESPONSE: Concur. We concur with the recommendation to train DoD contracting officers on access and use of CCR data. However, development of a stand-alone CCR training course or incorporation of CCR training into an established course curriculum are not currently considered viable options given the resources and time required to implement these alternatives. Instead, we intend to develop a CCR access and usage guide to facilitate contracting officer awareness and knowledge of CCR. We expect to develop this guide and distribute it to DoD contracting officers by April 1998.

Under Secretary of Defense for Acquisition and Technology Comments



ACQUISITION AND
TECHNOLOGY

DP/CPF

OFFICE OF THE UNDER SECRETARY OF DEFENSE

3000 DEFENSE PENTAGON
WASHINGTON DC 20301-3000

July 29, 1997

MEMORANDUM FOR: INSPECTOR GENERAL, DEPARTMENT OF DEFENSE

SUBJECT: Draft Audit Report on Federal Acquisition Computer
Network Central Contractor Registration Program
(Project No. 6CA-0070)

The attached summarizes our comments on the subject report.

My point of contact is Mr. Michael Mutty at (703) 697-6710.

Eleanor R. Spector
Director, Defense Procurement

Attachment



Under Secretary of Defense for Acquisition and Technology Comments

Final Report
Reference

COMMENTS ON DODIG DRAFT AUDIT REPORT ON
FEDERAL ACQUISITION COMPUTER NETWORK CENTRAL
CONTRACTOR REGISTRATION PROGRAM
(Project No. 6CA-0070)

Revised

Recommendation 2. We recommend that the Director, Defense Procurement (DDP) and the DoD Comptroller develop an information package on the Central Contractor Registration System and encourage the DoD Small Business Offices, finance offices and contracting offices to provide the packages to potential contractors.

DDP Response: Concur. DDP will, in coordination with Deputy Under Secretary of Defense(Logistics), Electronic Commerce Integration Office, develop an information package on the Central Contractor Registration System by December 1997.

Revised

Recommendation 3. We recommend that the Director, Defense Procurement and the DoD Comptroller:

a. Direct the Services' Senior Acquisition Executives to upgrade the computer equipment and software used by their respective contracting officers so that those users can access and use the Central Contractor Registration database.

DDP Response: Concur. The CCR Integrated Project Team (IPT) created by DDP will work with the Military Departments, Defense Agencies, and the Defense Finance and Accounting Office to ensure those organizations are able to access the CCR database. Direction has already been provided to the Military Departments to upgrade their computer systems. The current Defense Planning Guidance states "Components will install and operate local SPS infrastructure and support shared Defense Information Systems Network, Defense Message System, and similar services provided on a fee basis by DISA, with a goal towards full SPS deployment by the end of 2001."

b. Require that DoD contracting officers be trained to access and use the Central Contractor Registration database.

DDP Response: Concur. When the information package, discussed in the response to recommendation 2 is prepared, it will include a section on training for DoD contracting officers.

c. Publish information on the requirement to register for the Central Contractor Registration in the Commerce Business Daily.

DDP Response: Concur; however, DDP will publish the requirement for contractors to register in the CCR as a proposed Defense Federal Acquisition Regulation Supplement (DFARS) rule in the Federal Register rather than in the Commerce Business Daily.

Department of the Army Comments

Final Report
Reference



REPLY TO
ATTENTION OF

DEPARTMENT OF THE ARMY
HEADQUARTERS, MILITARY TRAFFIC MANAGEMENT COMMAND
5811 COLUMBIA PIKE
FALLS CHURCH, VA 22041-6060



11 AUG 1997

MTCS (36-2b)

MEMORANDUM FOR Inspector General, Department of Defense, ATTN: Mr. Kent E. Shaw,
400 Army Navy Drive, Arlington, VA 22202-2884

SUBJECT: Draft Audit Report "Federal Acquisition Computer Network Central Contractor
Registration Program" (Project No. 6CA-0070) dated 10 Jun 97)

1. This memorandum confirms discussions with you on 30 Jun 97 and provides Military Traffic Management Command (MTMC) comments on subject report.
2. MTMC is neither the contracting nor paying office for the personal property or freight carrier transactions discussed in the report. Accordingly, MTMC can not concur to recommendation 6a or 6c. The Defense Finance Accounting Service pays transportation bills and would be the logical addressee for recommendation 6a. Individual service transportation offices initiate the freight and personnel property shipment arrangements with individual carriers. As such, they would be the activity to prepare the "Individual Contracting Action Reports" addressed in recommendation 6c.
3. Concerning recommendation 6b, MTMC is actively working to assure that freight and personnel property carriers are made aware of and provide information needed by the Central Contract Registration database. As discussed in our 30 Jun 97 meeting, we were planning a publicity campaign to encourage carriers to complete the necessary registration data. This action was suspended due to new guidance in the joint Under Secretary Defense (Comptroller) and Director, Defense Procurement memorandum of 11 Jun 97 (Copy attached). MTMC will work within the guidance of this memorandum to populate the database.
4. MTMC point of contact for this response is Mr. Lawrence A. Powers, Chief of Internal Review and Audit Compliance Office. If there are additional questions, he may be contacted at (703)-681-6920.

FOR THE COMMANDER:

Atch

James L. Miller, Maj, S.D.S.
J. DOUGLAS FOYE
Colonel, GS
Chief of Staff

Printed on Recycled Paper

5.a. Deleted
5.c. Redi-
rected and
renumbered.



OFFICE OF THE SECRETARY OF DEFENSE
WASHINGTON, DC 20301

June 11, 1997



MEMORANDUM FOR DIRECTORS OF DEFENSE AGENCIES
DEPUTY FOR ACQUISITION AND BUSINESS MANAGEMENT,
ASN(RD&A)/ABM
DEPUTY ASSISTANT SECRETARY OF THE AIR FORCE
(CONTRACTING), SAF/AQC
DEPUTY ASSISTANT SECRETARY OF THE ARMY
(PROCUREMENT)
DEPUTY DIRECTOR (ACQUISITION), DEFENSE LOGISTICS
AGENCY
DIRECTOR, DEFENSE FINANCE AND ACCOUNTING SERVICE

SUBJECT: Central Contractor Registration

Several letters have been issued advising the acquisition and finance communities and defense contractors of DoD's intent to require that contractors be registered in the Central Contractor Registration (CCR) database to receive contract awards resulting from solicitations issued after September 30, 1997.

We have decided to delay implementation of that requirement while we take immediate steps to make it easier and quicker for contractors to register in the CCR. Rather than ask contractors to submit information that has already been provided to the government, we will first populate the CCR with information extracted from other databases. Contractors will then be asked to provide only the missing data elements and to verify the accuracy of existing data. We are also simplifying the process for registering through the World Wide Web, and we plan to reduce significantly the time it takes to validate registration data.

These actions will substantially improve the registration process and reduce the administrative burden for contractors. A firm date for imposing the requirement for contractors to be registered in the CCR cannot be established at this time. For planning purposes, the requirement for contractors to be registered in CCR as a prerequisite to receiving a DoD contract will be no earlier than March 31, 1998.

John J. Hamre
Under Secretary of
Defense (Comptroller)

Eleanor R. Spector
Director, Defense Procurement

cc: DSMC, Ft. Belvoir



Defense Information Systems Agency Comments



DEFENSE INFORMATION SYSTEMS AGENCY
701 S. COURTHOUSE ROAD
ARLINGTON, VIRGINIA 22204-2199



IN REPLY
REFER TO: Inspector General

30 July 1997


MEMORANDUM FOR INSPECTOR GENERAL, DEPARTMENT OF DEFENSE
ATTN: Director, Contract Management

SUBJECT: Comments to DODIG Draft Audit Report on Federal
Acquisition Computer Network Central Contractor
Registration Program (Project No. 6CA-0070)

1. The Agency's comments to the subject draft report are enclosed. We generally concur with the recommendations and, in some cases, have already initiated corrective actions. Our detailed management comments are enclosed.
2. The point of contact for this action is Ms. Sandra J. Sinkavitch, Audit Liaison on (703) 607-6316.

FOR THE DIRECTOR:

1 Enclosure a/s


RICHARD T. RACE
Inspector General

Quality Information for a Strong Defense

MANAGEMENT COMMENTS TO DODIG DRAFT REPORT ON
FEDERAL ACQUISITION COMPUTER NETWORK
CENTRAL CONTRACTOR REGISTRATION PROGRAM
(Project No. 6CA-0070)

We recommend the Director, Defense Information Systems Agency:

1. Upgrade the operating system used for its Central Contractor Registration (CCR) Program, to a version that complies with security requirements for C2-level security as required by DoD Directive 5200.28.

Response: Concur. The operating system used for CCR was upgraded to a C2-level security operating system on 20 July 1997.

2. Install a firewall that will restrict access to the Central Contractor Registration Interface computer, Megacenters Columbus, to authorized Value-Added Networks and gateways.

RESPONSE: Concur in Part. We do not believe the DODIG has a clear understanding of how the CCR operates; therefore, we offer the following comments for clarification.

There are two CCR machines commonly referred to as CCR and Central Contractor Registration Interface (CCRI). The CCRI machine is separated from the Electronic Commerce Processing Node (ECPN) and is, in fact, the firewall for the CCR machine. Although both machines physically reside in the Defense Megacenters Columbus, there is no physical connection between these two machines. Data that is collected via the WEB is "pushed" from the CCRI machine on a daily basis to the CCR machine. This is done by utilizing a X-12 standard 838 transaction set routed over the ECPN for delivery to the CCR machine.

The statement concerning "to authorized Value-Added Networks and gateways" also needs to be clarified. The accessibility of CCR data is in no way strictly limited to VANs and gateways. There is a segment of data that is accessible to the "public", procurement officials, etc. To ensure this data is protected, software has been installed to limit the particular view of the data by utilizing userid/passwords assigned to the users. This function is performed and controlled by the Defense Logistics Service Center (DLSC) under the customer support agreement. To safeguard the data from "hackers", this query capability is directed to a "copy" of the master database.

Enclosure

This copy resides on the CCRI machine --again used as a firewall for the protection of the CCR master database (which physically resides on the CCR machine). We believe we have adequate firewall protection and request the DODIG reconsider the recommendation.

3. Install security software for its Internet web server that will encrypt registration data submitted by its contractors while it is enroute to the server.

RESPONSE: Concur. DISA is currently using VeriSign encryption technology to provide positive identification of the site submitting the data. This product also provides an adequate level of security to ensure the information that is transmitted from the contractor to the WEB site remains unaltered during transmission. (Note: The submitter of the data has a choice of utilizing the VeriSign encryption technology or choosing to send the data via the WEB in clear text.) Once received at the CCRI, use of "userid/passwords" will preclude data from being changed by unauthorized users. These procedures provide what DISA feels is an adequate level of security for contractor data.

Audit Team Members

This report was prepared by the Contract Management Directorate, Office of the Assistant Inspector General for Auditing, DoD.

Paul J. Granetto
Kimberley A. Caprio
Kent E. Shaw
Johnetta R. Colbert
Young J. Jin
Robert E. Beets
William C. Coker
Awanda Grimes
Sylvia Powell
Ana M. Myrie

INTERNET DOCUMENT INFORMATION FORM

A . Report Title: Federal Acquisition Computer Network Central Contractor Registration (CCR) Program

B. DATE Report Downloaded From the Internet: 10/07/99

C. Report's Point of Contact: (Name, Organization, Address, Office Symbol, & Ph #): OAIG-AUD (ATTN: AFTS Audit Suggestions)
Inspector General, Department of Defense
400 Army Navy Drive (Room 801)
Arlington, VA 22202-2884

D. Currently Applicable Classification Level: Unclassified

E. Distribution Statement A: Approved for Public Release

F. The foregoing information was compiled and provided by:
DTIC-OCA, Initials: __VM__ Preparation Date 10/07/99

The foregoing information should exactly correspond to the Title, Report Number, and the Date on the accompanying report document. If there are mismatches, or other questions, contact the above OCA Representative for resolution.